Algorithmes et Protocoles Cryptographiques

Chapitre1: Définitions et concepts de base

M. Mahmoud TOUNSI
Mme. Arbia RIAHI

INDP2
SUPCOM, 2022

Organisation du module

- Volume horaire : 21h, cours intégré.
- Modalité d'examen …..
- Objectifs:
  - Introduction à la cryptographie (pré-requis : mathématiques élémentaires).
  - Application de concepts cryptographiques aux protocoles de communication (prot. d'authentification, de confidentialité, à connaissance zéro…).

À méditer

La sécurité basée sur autre chose que les principes cryptographiques restera un bazar (*will remain a mess*).

Shamir

Si vous pensez que la cryptographie est la solution à votre problème alors vous ne comprenez pas la cryptographie et vous ne comprenez pas votre problème

attribué à Lampson et/ou Needham

Problèmes de sécurité

- Indiscrétion (Eavesdropping)

– l’information n’est pas altérée, mais sa confidentialité est compromise.

– espionnage passif.

– Ex : récupération du N° d’une carte de crédit et de son code confidentiel.

- Falsification (Tampering)

– l’information en transit est modifiée ou remplacée avant d’être remise à son destinataire.

– espionnage actif.

– ex : changer le montant d’un virement bancaire.

Problèmes de sécurité

- Imitation (Impersonation)
  – Mystification (Spoofing)
    ✓ une personne ou une entité se fait passer pour une autre
    ✓ ex : utilisation frauduleuse de l'adresse e-mail d'une Personne
  – Imposture (Misrepresentation)
    ✓ une personne ou une organisation prétend être ce qu'elle n'est pas
    ✓ ex : un site prétend commercialisé des fournitures informatiques alors qu'il ne fait qu'encaisser les paiements par cartes de crédit sans jamais livrer de marchandises.

Plan

- Introduction
- Définitions et concepts de base
- Cryptosystèmes à clés symétriques
- Cryptosystèmes à clés asymétriques
- Fonctions de hashage
- Protocoles cryptographiques
- Cryptanalyse

Introduction (1)

- Une longue histoire, un art et une activité mystérieuse.
- Facteurs de changements :
  - Introduction des ordinateurs, intérêt commercial, consolidation mathématique.
  - Une variété d'ingrédients techniques : théorie des nombres, probabilités, théorie de l'information et codage, théorie de la complexité du calcul.
- La cryptographie est de plus en plus utilisées dans:
  - Confidentialité des e-mail.
  - Protection des accès aux réseaux(LAN).
  - Sécurité des transactions bancaires.
  - Cartes à puces.
  - Réseaux privés virtuels.
  - ...

Introduction (2)

- Cryptographie : Science mathématique permettant d'effectuer des opérations sur un texte intelligible afin d'assurer une ou plusieurs propriétés de la sécurité de l'information.
- But : fournir aux messages/communications les propriétés suivantes:
  - **La Confidentialité :** afin d'assurer le secret du message qui ne peut être lu que par le destinataire légitime.
  - **L'Authentification** afin de s'assurer de l'identité de l'expéditeur.
  - **L'Intégrité** afin d'assurer que le message n'a pas été modifié ou corrompu durant la communication.
  - **La Non-répudiation** afin de 'lier' l'expéditeur authentifié au message.

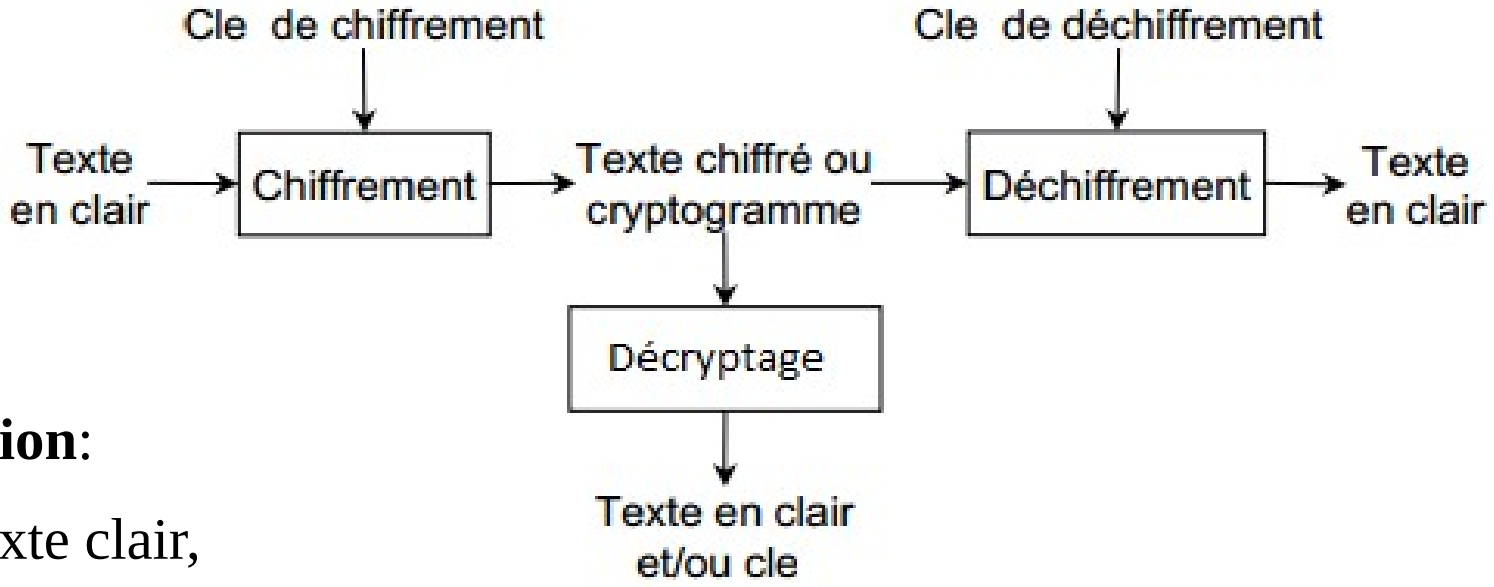
Introduction (3)

- Place du chiffrement : trois niveaux possibles,
  - Liaison : mise en place de boîtes noires sur les supports de transmission ;
  - Réseau : des équipements spécialisés sont placés sur chacun des sites, au niveau des routeurs ;
  - De bout en bout : seules les données constituant l'information transmise sont chiffrées. Il est mis en œuvre dans les applications du modèle TCP/IP.
- L'ensemble repose, dans tous les cas, sur un algorithme donné, une clé ou un couple de clés associées et un mécanisme de distribution des clés.

Définitions générales

- Chiffrer : transcrire, à l'aide d'un algorithme paramétrable un message clair en une suite incompréhensible de symboles.
- Texte en clair : le message à chiffrer.
- Texte chiffré : le résultat du chiffrement.
- Déchiffrer : retrouver le texte en clair à partir du texte chiffré à l'aide d'un algorithme paramétrable.
- Clé : le paramètre des algorithmes de chiffrement et de déchiffrement.
- Décrypter : retrouver le texte en clair à partir du texte chiffré sans la clé.
- Cryptographie : science du chiffrement.
- Cryptanalyse : science du décryptage
- Cryptologie : cryptographie et cryptanalyse
- Cryptosystème : ensemble des méthodes de chiffrement et de déchiffrement utilisables en sécurité.

Modèle de chiffrement



Notation:

M: Texte clair,

C: Texte chiffré

E(M): Opération de chiffrement de M,

D(C): Opération de déchiffrement de C.

Il faut évidemment que **D(E(M))=M**

Principe de Kerckhoff

Kerckhoff a introduit plusieurs principes :

1) Le système doit être matériellement, sinon mathématiquement, indéchiffrable.
2) Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.
3) La clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants.
4) Il faut qu'il soit applicable à la correspondance télégraphique.
5) Il faut qu'il soit portatif et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.
6) Il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Principes de Shannon

Un chiffrement doit apporter de la confusion et de la diffusion:

- Confusion : Il n'y a pas de relation algébrique simple entre le clair et le chiffré. En particulier, connaître un certain nombre de couples clair-chiffré ne permet pas d'interpoler la fonction de chiffrement pour les autres messages. Tout le contraire d'un chiffrement affine.
- Diffusion : La modification d'une lettre du clair doit modifier l'ensemble du chiffré. On ne peut pas casser le chiffrement morceau par morceau. Tout le contraire d'un chiffrement mono-alphabétique.

En résumé : principes de la cryptographie moderne

- Principe de Kerchkoff : Tous les algorithmes doivent être publics; seules *les clés sont secrètes*.
- Principes de Shannon : Un chiffrement doit apporter de la confusion et de la diffusion,

- Conséquences :
  - le véritable secret réside dans la clé.
  - l'algorithme public doit être fort et la clé doit être longue.
- Problèmes :
  - quelle longueur de clés choisir ?
  - quelle fréquence de renouvellement des clés choisir ?
  - comment s'échanger les clés ?

Cryptosystèmes

Cryptosystème : l'ensemble des clés possibles des textes clairs et chiffrés possibles associés à un algorithme donné.

- Les algorithmes de chiffrement/déchiffrement doivent atteindre des vitesses de chiffrement élevés et utiliser peu d'espace mémoire.
- Redondance : on ne doit pas pouvoir créer des textes "ressemblant" à des textes chiffrés.
- Fraîcheur : le destinataire peut s'assurer qu'un message est récent.
- On distingue deux grandes familles de cryptosystèmes :
  - Cryptosystèmes à clés symétriques
  - Cryptosystèmes à clés asymétriques

Le théorème du secret parfait

- Pour étudier un cryptosystème, Shannon introduit un modèle de sécurité probabiliste : un attaquant peut tomber par hasard sur la bonne clé.

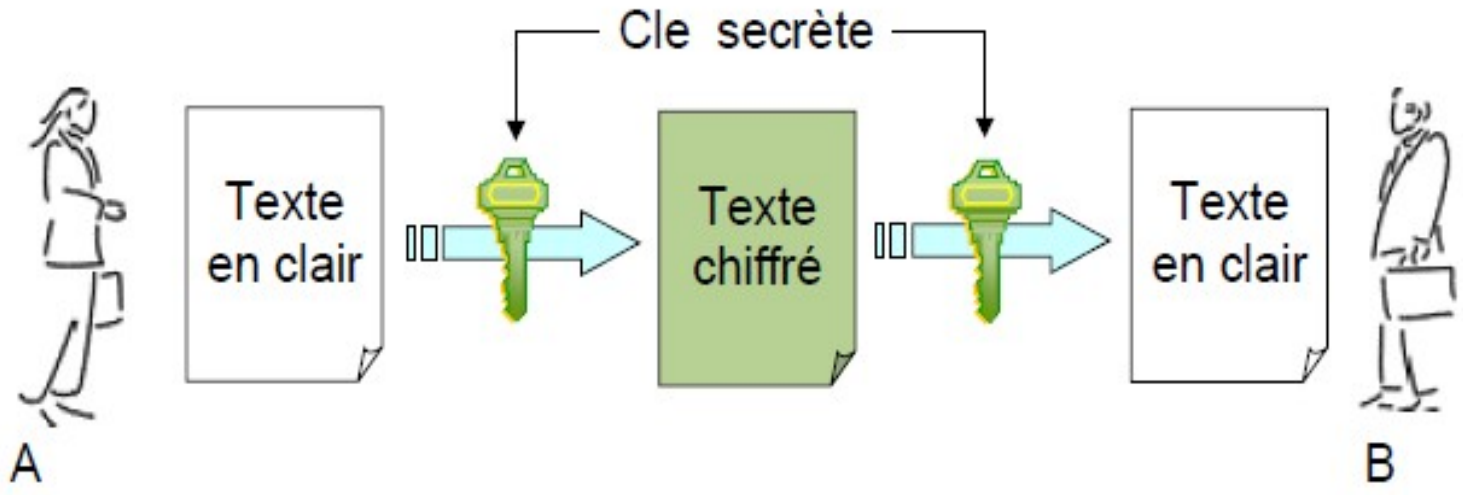
=> L'essentiel est que les interceptions de messages n'augmentent pas ses chances.

- **Définition** : Un cryptosystème est dit à **secret parfait** si la réception d'un chiffré ne donne aucune information sur le clair dont il est issu

$$\forall\ m, c, Pr(m \mid c)=Pr(m)$$

Pr(m | c), la probabilité d'obtenir *m* le texte en clair sachant le texte chiffré *c*.

Cryptosystèmes à clés symétriques (1)



- Caractéristiques:
  - Clés identiques: clé de chiffrement=clé de déchiffrement= clé secrète.
  - Clé secrète!

Cryptosystèmes à clés symétriques (2)

- Chiffrement par substitution : chaque lettre ou groupe de lettres est remplacé par une autre lettre ou un autre groupe de lettres.
- Chiffrement par transposition : on modifie l’ordre des lettres d’un texte en clair.
- La plupart des algorithmes de chiffrement symétriques ne sont qu’un mélange savant de substitutions et transpositions (ex : DES, AES).

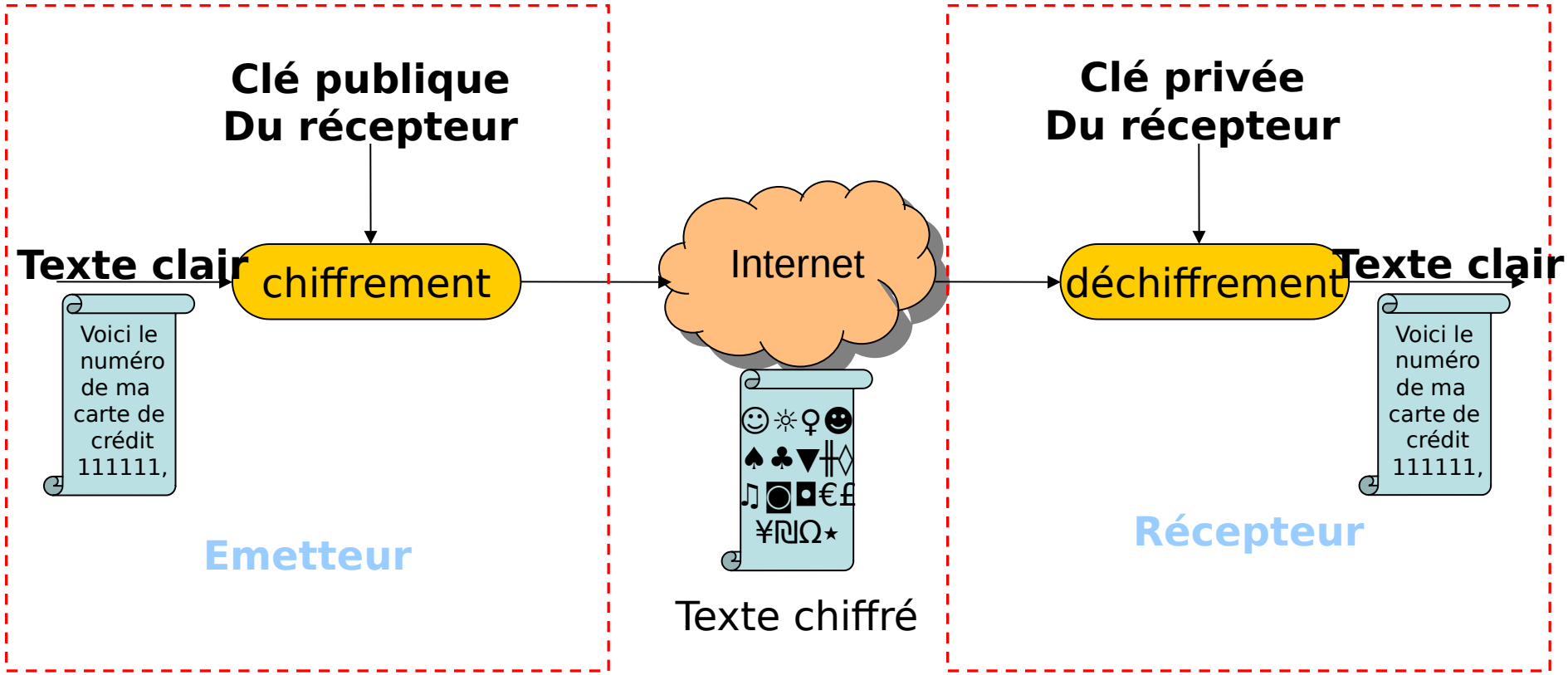
Cryptosystèmes à clés symétriques (3)

- Algorithmes :
  - Chiffrement en continu / par flux / par flot / à la volée (*Stream Cipher*)
    - Agissant sur un bit à la fois (en général XOR entre le texte en clair et la clé), ex. RC4.
  - Chiffrement par bloc (*Bloc Cipher*)
    - Opère sur le texte en clair par blocs de taille fixe (64b, 80b, 128b…)
    - Ex. DES, 3DES, IDEA, AES, CAST, etc.
- Performances: Chiffrement très rapide.
- Problèmes
  - Nombre de clés: pour *n* entités ? Réponse …….
  - Distribution des clés:
    - Opération critique.
    - Doit s'effectuer de manière sécurisée (voire manuellement).

Cryptosystèmes à clés asymétriques (1)

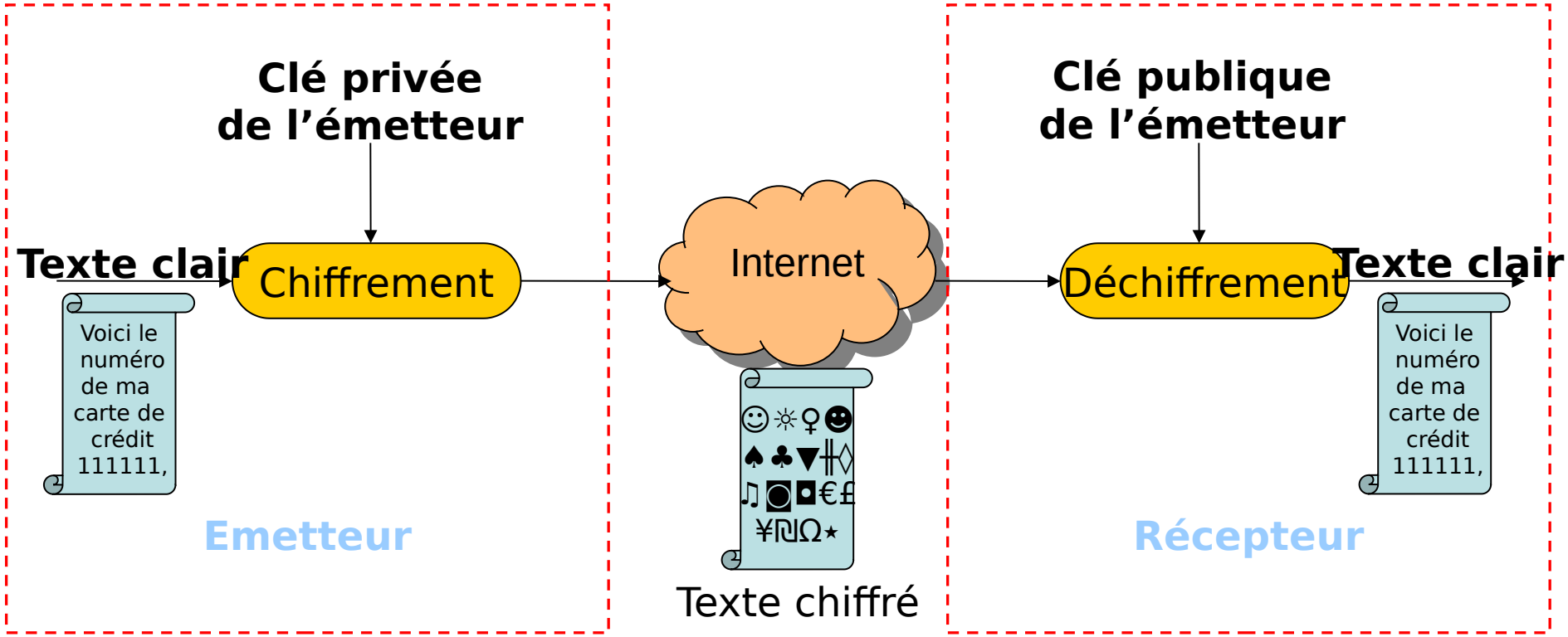
- Pour chaque entité : une clé publique (diffusée), une clé privée (gardée secrète).
- Algorithmes :
  - Diffie & Hellman (1976), RSA (1978), ELGAMEL…
  - Basés sur des problèmes mathématiques difficiles à résoudre (log. Discret, factorisation de grands nombres en entiers premiers).
- Performances: Chiffrement beaucoup lent.
- Nombre de clés (pour n entités) : 2n clés (n paires).
- Distribution des clés:
  - Facilitée car il n’y a plus d'échange de clés.
  - Secret nécessaire : la clé privée est conservée par les entités.
  - Seule la clé publique est échangée. Sa connaissance ne permet pas de déduire la clé privée

Cryptosystèmes à clés asymétriques (2)



Ce mode assure la confidentialité

Cryptosystèmes à clés asymétriques (3)



Ce mode assure la non-répudiation et l'authentification

Algorithmes de hashage

- Troisième grande famille d'algorithmes utilisés en cryptographie.
- Principe: conversion d'un texte original de longueur quelconque en un message de longueur fixe (en général de longueur inférieure).
- En cryptographie : utiliser le message hashé comme empreinte digitale du message original.
- Propriétés
  - *Unidirectionnels* : Le calcul de H(M) est rapide (M connu), mais l'opération inverse est impossible, c-à-d de trouver (en un temps raisonnable) M sachant H(M).
  - *Sans collision*: Il est difficile de générer 2 messages originaux M1et M2 tels que H(M1)=H(M2).
  - Longueur fixe du résultat.
- H (x) est appelé l'empreinte (ou aussi : condensé, condensat, haché, hash) du texte x.

Algorithmes de hashage

- La contrainte d'injectivité de la fonction de hachage H ne peut être satisfaite car en entrée un ensemble infini de message vers un ensemble fini de hash (2^n éléments),
- Par conséquent, il existe nécessairement x ≠ x' tel que H(x) =H(x') : « une collision ».
- Donc tout ce que l'on peut demander à f , c'est qu'il soit difficile de fabriquer des collisions.
- Pour satisfaire la contrainte précédente, il faut que *n* soit suffisamment grand afin d'éviter l'attaque par anniversaires.

Paradoxe des anniversaires (1)

- On se pose la question de savoir combien doit-on réunir de personnes afin d'avoir plus de 50% de chances d'avoir au moins deux personnes nées le même jour de l'année (pour simplifier, on suppose toutes les années non bissextiles, ce qui ne change guère le résultat).
- La réponse, très contre-intuitive, est 23. Si on réunit 50 personnes, la probabilité est de 97,04% et, pour 80 personnes, elle est de 99,99%, une quasi certitude.
- Question : cherchez la formule !

Paradoxe des anniversaires (2)

P(deux personnes ont le même anniversaire) = 1 – P(k personnes ont des anniversaires différents)

= 1 – 365/365 x 364/365 x ….x (365 – k)/365

= 1 – A(365, k)/365^k

=1 – 365! /((365 – k)! x 365^k)

$$= 1 - \frac{365!}{(365-k)!}\frac{1}{365^k}$$

=> Avec ce paradoxe, il suffit de faire des recherches sur $2^{N/2}$ pour avoir des collisions.

Attention : N doit être assez grand

Paradoxe des anniversaires (3)

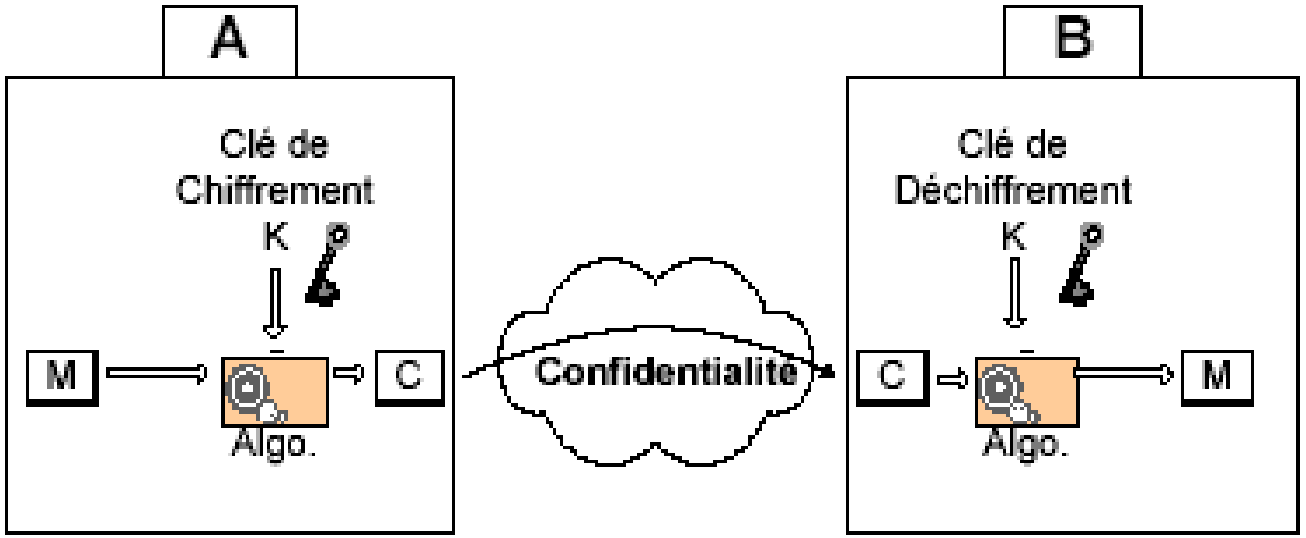
- Soit f une fonction de hachage. On choisit aléatoirement : x_1; x_2; ……. jusqu'à ce qu'on trouve une collision, c'est à dire x_i , x_j avec $i \neq j$ et tels que $f(x_i) = f(x_j)$.
- Méthode très efficace si la taille de l'empreinte est trop petite.
- Taille de l'empreinte : 64 bits. Il faut environ $4{,}2 \times 10^9$ essais pour avoir au moins 75% de chances de découvrir une collision (on suppose que toutes les empreintes sont équiprobables). À la portée d'un PC!
- Il faut également comparer ce nombre au nombre d'empreintes possibles, à savoir Environ $1{,}8 \times 10^{19}$.
- Avec une empreinte de 512 bits et pour une même probabilité, il faut au moins $1{,}15 \times 10^{77}$ essais, ce qui est hors de portée d'un PC.

Protocoles cryptographiques

- Dès que plusieurs entités sont impliquées dans un échange de messages sécurisés, des règles doivent déterminer l'ensemble des opérations cryptographiques à réaliser, leur séquence, afin de sécuriser la communication : C'est ce que l'on appelle les **protocoles cryptographiques**.
- Que signifie sécuriser un échange?
  - Assurer les 4 propriétés fondamentales :
    - Confidentialité
    - Authentification
    - Intégrité
    - Non-répudiation

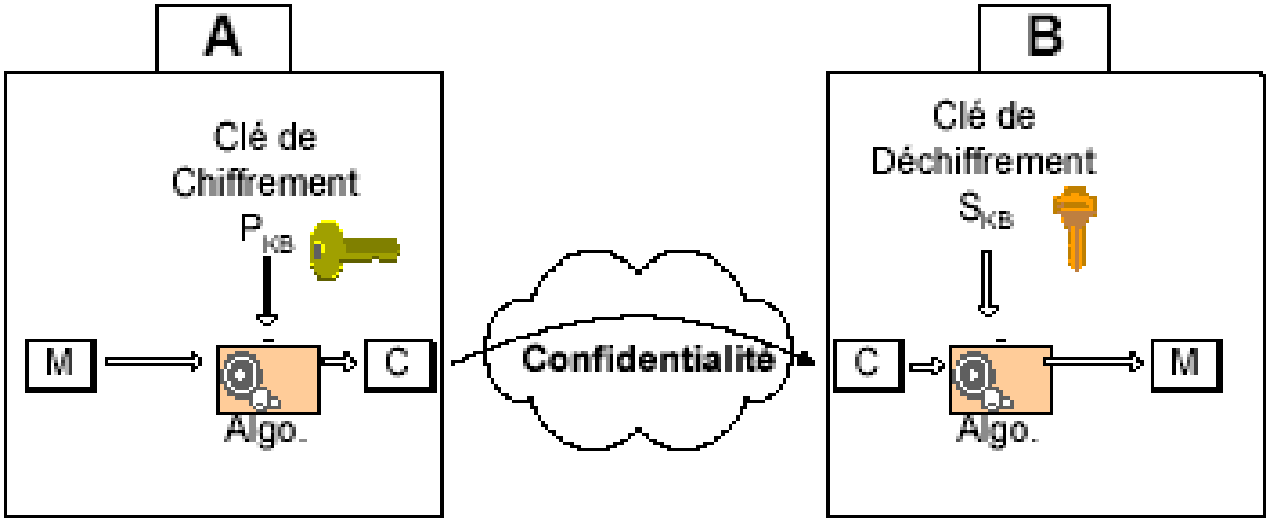
Confidentialité

- A l'aide de cryptosystèmes à clés symétriques:
  - La même clé secrète est utilisée pour E(M) et D(C)
  - Échange préalable et sécurisé de la clé K entre A et B.



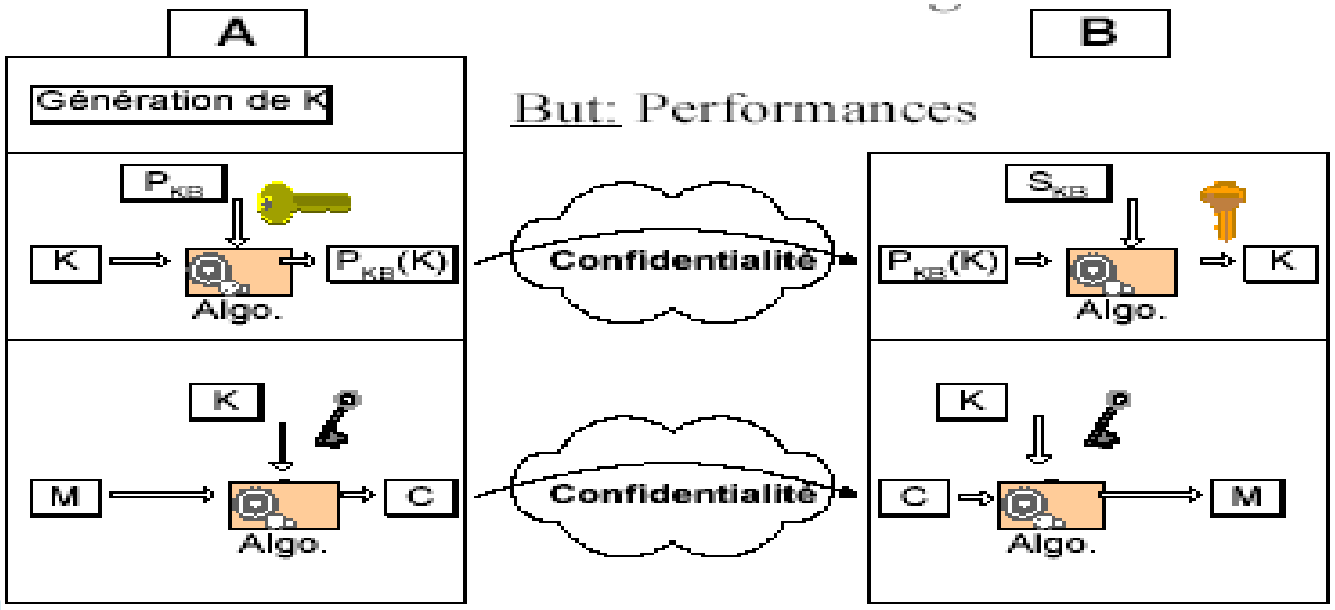
Confidentialité

- A l'aide de cryptosystèmes à clés publiques.
  - Chaque entité possède sa paire de clés PKA, SKA/ PKB, SKB.



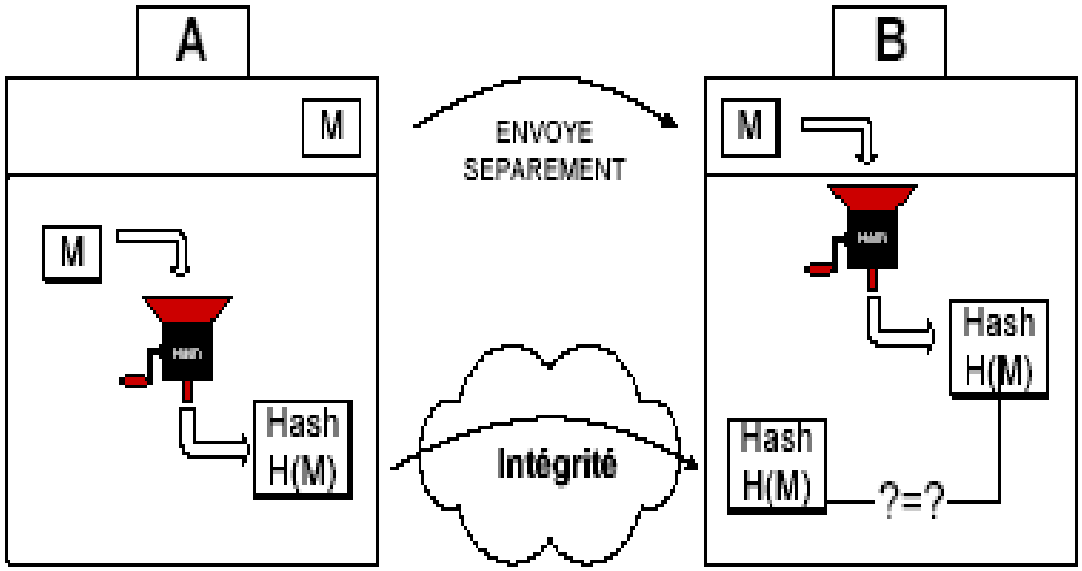
Confidentialité

- A l'aide de cryptosystèmes hybrides.
  - Cryptosystème à clés publiques pour l'échange confidentiel de la clé (de session) K.
  - Cryptosystème à clés symétriques pour l'échange confidentiel du message.



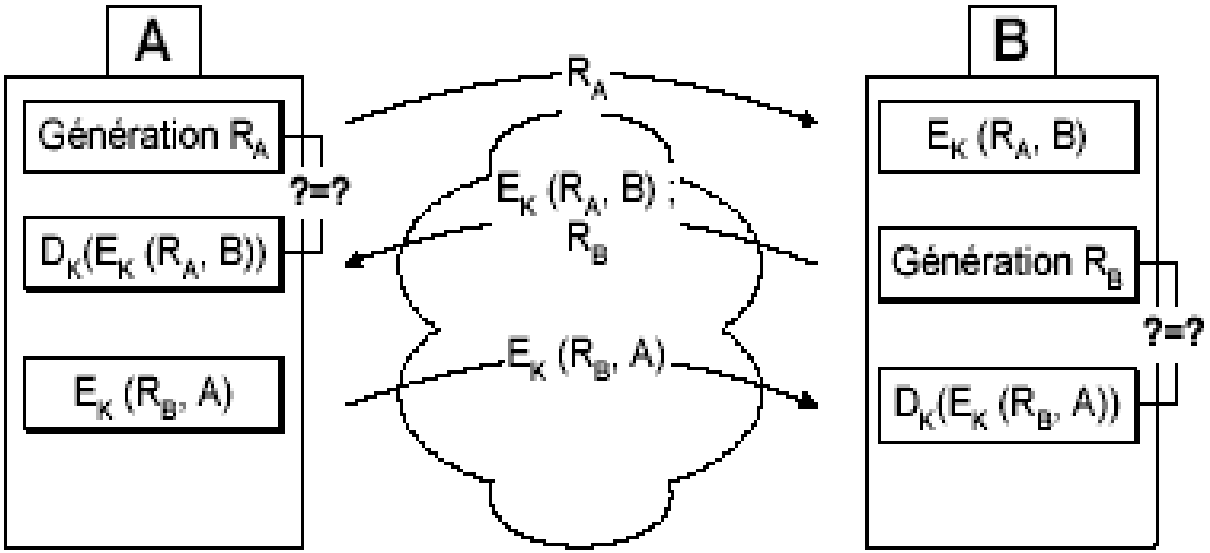
Intégrité

- Vérification qu'un message n'a pas été altéré durant la communication.
- On utilise les fonctions de hashage.



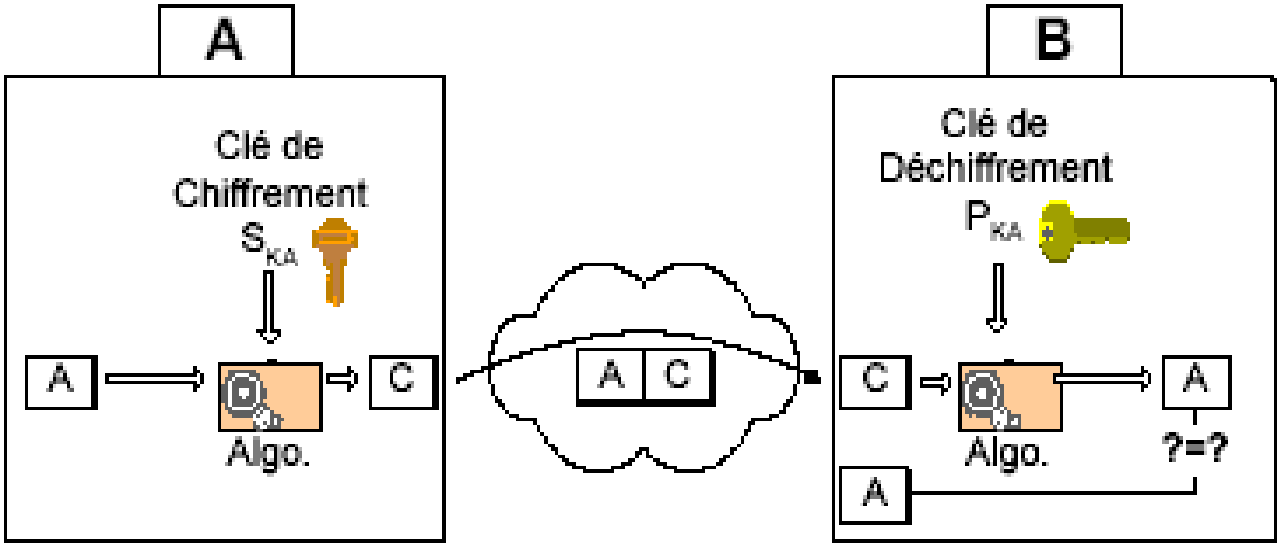
Authentification

- Des parties de la communication.
  - A l'aide d'un cryptosystème à clés symétriques.
    - Si on suppose que A et B partagent une même clé secrète K



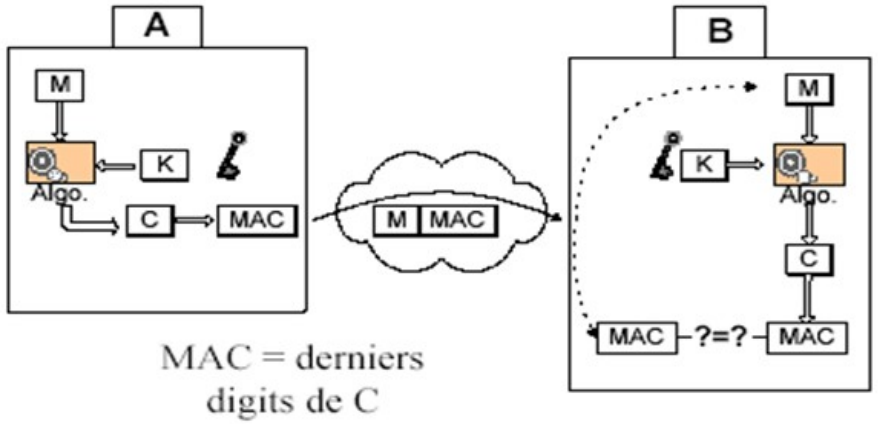
Authentification

- A l'aide d'un cryptosystème à clés publiques.
  - Chaque partie possède une paire de clés publique/privée (PKA/SKA, PKB/SKB).

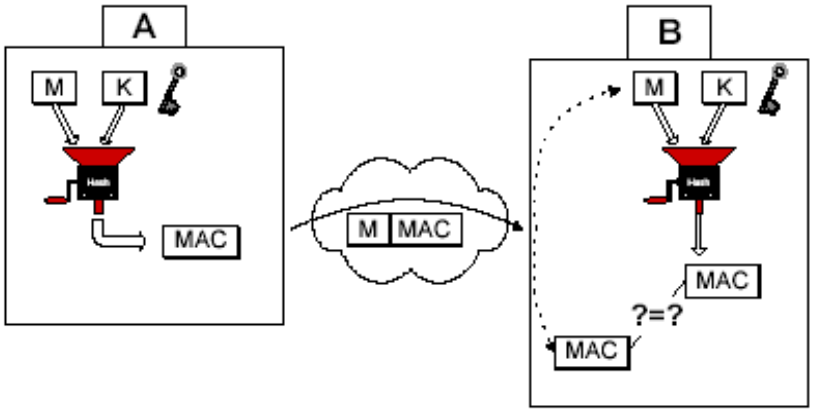


Authentification

- Du message :
  - À l'aide d'un MAC (*Message Authentication Code*).
  - Un MAC peut être généré de deux manières:
    - A l'aide d'un cryptosystème symétrique.
    - A l'aide d'une fonction de hashage.

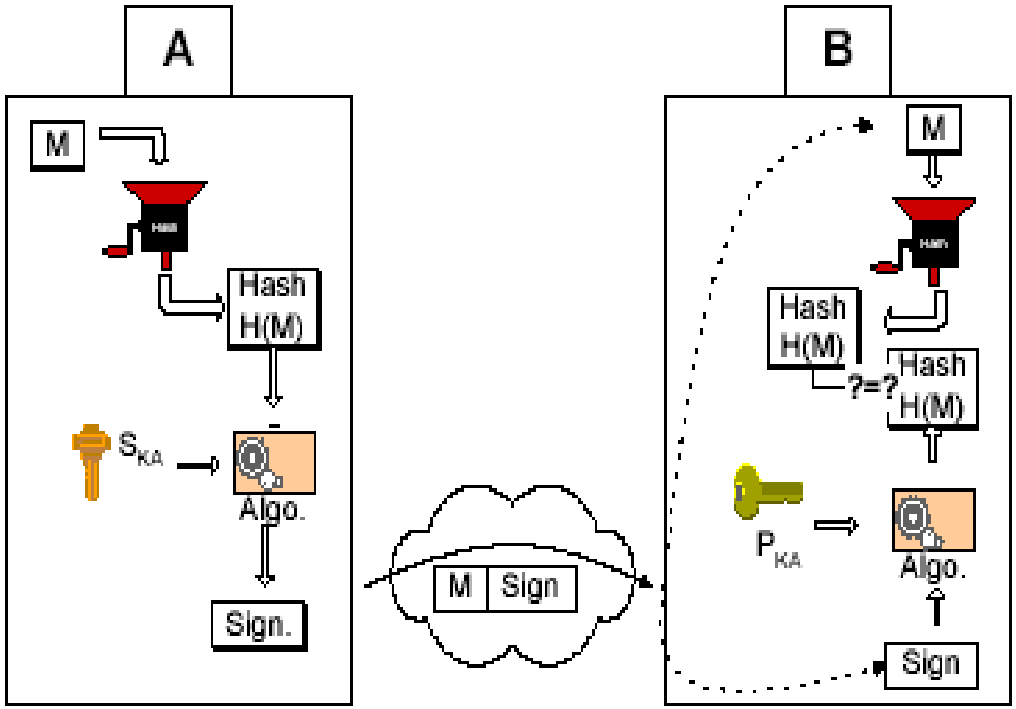


MAC = derniers digits de C

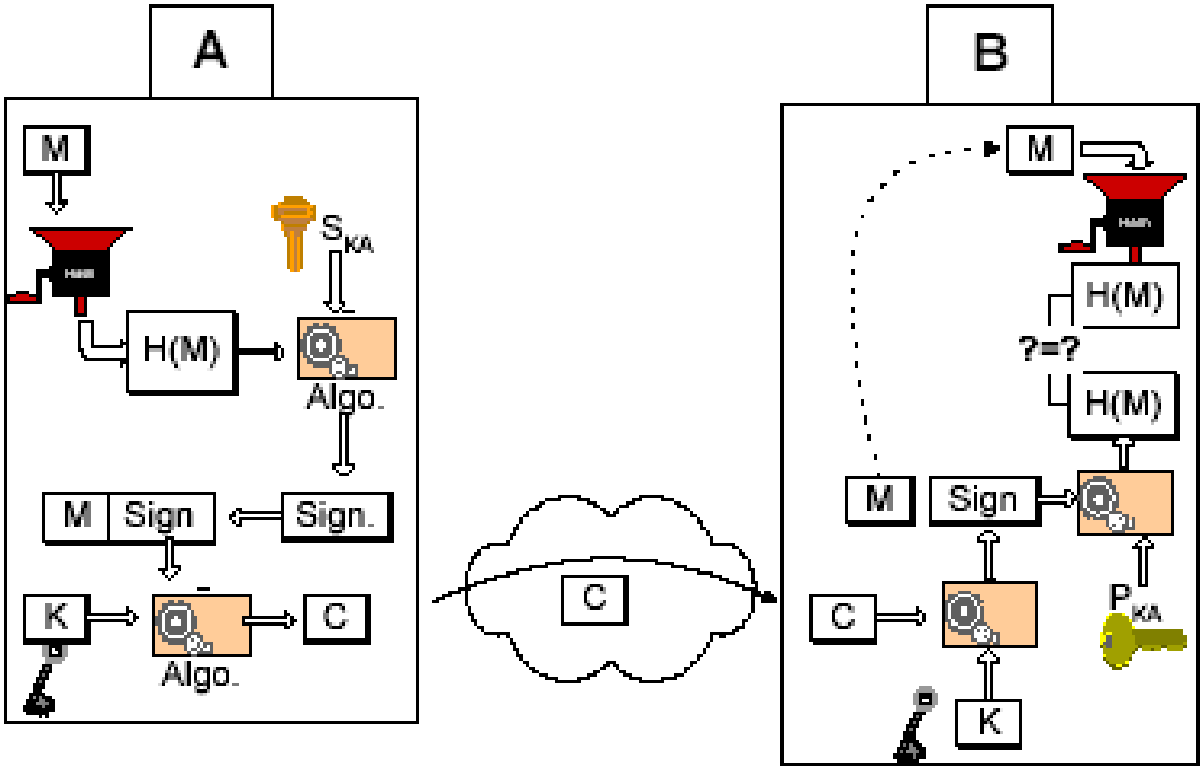


Authentification

- Du message.
  - A l'aide d'une signature électronique.
  - Propriétés :
    - Authentique
    - Infalsifiable
    - Non-réutilisable
    - Inaltérable
    - Non-répudiable



Enfin tous les services de sécurité garantis !



Cryptanalyse : les attaques (1/4)

- L'attaque à texte chiffré seulement (cipher text only):
  - Le cryptanalyste dispose du texte chiffré de plusieurs messages, avec le même algorithme.
  - Objectif : retrouver le plus grand nombre de messages clairs possibles, ou retrouver la ou les clés qui ont été utilisées.
- L'attaque à texte clair connu (known plaintext):
  - Le cryptanalyste a accès aux textes chiffrés de plusieurs messages, et aux textes clairs correspondants.
  - Objectif : retrouver la ou les clés utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer d'autres messages chiffrés avec ces mêmes clés.

Cryptanalyse : les attaques (2/4)

- L'attaque à texte clair choisi (chosen plain text):
  - Le cryptanalyste a accès aux textes chiffrés et aux textes clairs correspondants, et peut choisir les textes en clair.
  - Cette attaque est plus efficace que l'attaque à texte clair connu, car le cryptanalyste peut choisir des textes en clair spécifiques qui donnent plus d'informations sur la clé.
- L'attaque à texte chiffré connu (chosen cipher text)
  - Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer. Les textes déchiffrés lui sont alors fournis.
  - Par exemple: le cryptanalyste a un dispositif qui ne peut être désassemblé et qui fait du déchiffrement automatique. Sa tâche est de retrouver la clé.

Cryptanalyse : les attaques (3/4)

- L'attaque adaptative à texte chiffré choisi (adaptive chosen ciphertext attack) :
  - Attaque à texte chiffré choisi où le choix du texte chiffré peut dépendre du texte en clair reçu précédemment.

- L'attaque exhaustive ou attaque par force brute (brute force attack) :
  - L'attaquant essaie toutes les combinaisons possibles des clés jusqu'à l'obtention d'un texte clair. Cette attaque est la plus coûteuse en temps de calcul et en mémoire à cause de la recherche exhaustive.

Cryptanalyse : les attaques (4/4)

- Attaques physiques:
  - Essayer de reconstituer la clé secrète par exemple en espionnant la transmission entre le clavier de l'ordinateur et l'unité centrale ou en mesurant la consommation électrique du microprocesseur qui effectue le décodage du message ou encore en mesurant son échauffement. Ensuite on essaye de remonter de ces données physiques aux clés de chiffrement et déchiffrement.
  - Une méthode pour résister à ce type d'attaque sont les protocoles de preuve sans transfert de connaissance (zero-knowledge proof)

Travaux demandés

- Exemple d’attaque physique.
- Résumé des théorèmes du secret parfait ou Systèmes cryptographiquement sûrs de shannon.
- Schéma de Feistel